UNITED STATES PATENT AND TRADEMARK OFFICE

MN

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/726,595	12/04/2003	Myungsun Kim	KIMM3005/EM	6978

23364 7590 07/19/2007

BACON & THOMAS, PLLC
625 SLATERS LANE
FOURTH FLOOR
ALEXANDRIA, VA 22314

EXAMINER	
LAFORGIA, CHRISTIAN A	
ART UNIT	**PAPER NUMBER**
2131	

MAIL DATE	DELIVERY MODE
07/19/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/726,595	KIM ET AL.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2 and 7* is/are rejected.

7)☒ Claim(s) *3-6* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-7 have been presented for examination.

Priority

2. Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d).

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application Publication No. 2003/0041262 A1 to Kon, hereinafter Kon, in view of U.S. Patent Application Publication No. 2003/0182554 A1 to Gentry et al., hereinafter Gentry.

5. As per claims 1 and 7, Kon teaches an anonymous fingerprinting method using a bilinear Diffie-Hellman problem, in a fingerprints embedment system that includes three participants, comprising the steps of:

(b) registering information on the first participant (i.e. user equipment) to a third participant (i.e. authentication organization server) based on the system parameters and the public and the secret key of the first participant, wherein the third participant issues a certificate based on the information on the first participant (Figures 1 [block 4], 3B, 5-7 [block 4], paragraph 0010, i.e. authentication organization server issues the open key certificate for the authentication of at least one user);

(c) at the second participant (i.e. content distributing server), authenticating a fairness of the first participant based on the certificate (paragraph 0021, i.e. authentication of the users is performed by the content distribution servers);

(d) embedding fingerprints into a digital content to be bought by the first participant (paragraphs 0022, 0031, i.e. electronic watermark inserted in a content by each content distributing server); and

(e) when an illegal duplicate of the digital content or an illegally redistributed duplicate is found, identifying a traitor, who illegally duplicates the digital content or redistributes the illegally duplicated digital content, with the first participant based on the fingerprints embedded in the digital content (paragraph 0061 i.e. content protection). As the Applicant admits on page 2 of the Specification, under "Background of the Invention," that conventional fingerprinting methods allows a merchant to embed information on the buyer in a digital content such that a merchant can examine an illegal duplicate or an illegally redistributed duplicate to trace an illegal buyer or re-distributor based on the buyer's information embedded in the illegally redistributed content.

6. Kon does not teach introducing system parameters shared by a first and a second participant, storing the system parameters in a memory of each of the first and the second participant and generating a public key and a secret key of the first participant.

7. Gentry discloses introducing parameters shared by a first and second participant (paragraph 0008) and generating a public key (paragraph 0035) and private key (paragraph 0040).

8. It would have been obvious to one of ordinary skill in the art at the time the invention was made to introduce system parameters shared by a first and a second participant, store the parameters in memory, and generate a public and private key, since Gentry states at paragraph 0007 that it provides a way to avoid key escrow and secure against passive attacks based on interception of messages between the two participants.

9. Regarding claim 2, Gentry teaches wherein the step (a) includes the steps of: (al) generating G1 and G2, wherein G1 is an elliptic curve group and G2 is a cyclic multiplicative group; (a2) taking a generator P out of the cyclic multiplicative group G2; (a3) calculating a bilinear map e on the groups G1 and G2 as follows: e : G1 x G1 -> G2, (a4) storing the system parameters in a storage medium of the third participant and opening the system parameters so that the first and the second participant can use them, wherein the system parameters has G1, G2 and P; (a5) selecting a secret key of the first participant out of G2, wherein the secret key of the first participant is formed of sl, s2 and s3; and (a6) calculating a public key YB of the first participant as follows: $Y_B = e(P, P)^{s1s2s3}$ (paragraphs 0021-0023).

Allowable Subject Matter

10. Claims 3-6 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

11. There are no teachings in the prior art of the claimed pseudonym keys used in conjunction with a content distribution system with Bilinear Diffie-Hellman. Since no teachings or motivation can be found to incorporate the pseudonym keys with a content distribution system with Bilinear Diffie-Hellman, claims 3-6 are therefore novel and non-obvious.

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

13. The following patents are cited to further show the state of the art with respect to bilinear Diffie-Hellman, such as:

United States Patent Application Publication No. 2003/0179885 A1 to Gentry et al., which is cited to show examples of bilinear Diffie-Hellman.

United States Patent Application Publication No. 2003/0081785 A1 to Boneh et al., which is cited to show examples of bilinear Diffie-Hellman.

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

15. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

16. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
Patent Examiner
Art Unit 2131

clf